FortiClient EMS - QuickStart Guide

Version 1.2.5

FORTINET DOCUMENT LIBRARY
http://docs.fortinet.com

FORTINET VIDEO GUIDE
http://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTIGATE COOKBOOK
http://cookbook.fortinet.com

FORTINET TRAINING SERVICES
http://www.fortinet.com/training

FORTIGUARD CENTER
http://www.fortiguard.com

END USER LICENSE AGREEMENT
http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

March 8, 2018
FortiClient EMS 1.2.5 QuickStart Guide
04-125-408698-20180308

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-03-08	Initial release.

Introduction

This guide describes how to install and set up FortiClient Enterprise Management Server (EMS) for the first time. FortiClient EMS is used to deploy and manage FortiClient endpoints.

An informative video introducing you to FortiClient EMS is available in the Fortinet Video Library.

Supported installation platforms

You can install FortiClient EMS on the following platforms:

- Microsoft Windows Server 2008 R2 or newer

For information about minimum system requirements and supported platforms, see the *FortiClient EMS Release Notes*, available in the Fortinet Document Library.

Required services and ports

You must ensure required ports and services are enabled for use by FortiClient EMS and its associated applications on your server. The required ports and services enable FortiClient EMS to communicate with endpoints and servers running associated applications. You do not need to enable ports 8013 and 10443 as the FortiClient EMS installation opens these.

Communication	Service	Protocol	Port
FortiClient endpoint/FortiClient Telemetry	File transfers	TCP	8013 (default)
FortiClient big data communication • Used for FortiClient to upload large amounts of data (100+ KB of data per connection) to FortiClient EMS.	File transfers	TCP	8014 (default)
Computer browser service • Allows FortiClient endpoints to automatically connect to EMS. The computer browser service is not needed if an Active Directory is used or endpoint users can manually connect FortiClient to EMS.	Enabled		

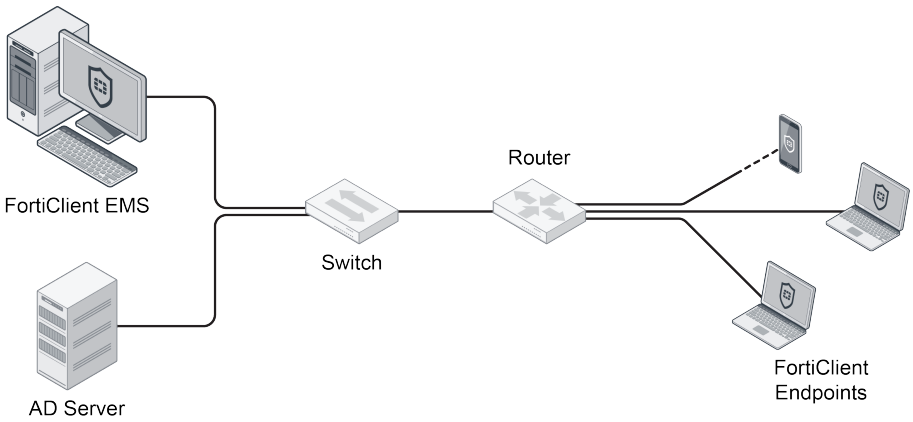
Communication	Service	Protocol	Port
Samba (SMB) service • FortiClient EMS uses the SMB service during FortiClient deployment.	Enabled		445
Distributed Computing Environment / Remote Procedure Calls (DCE- RPC) • The EMS server connects to endpoints using RPC for FortiClient deployment.	Enabled		135
Active Directory server connection	When used as a default connection		389 (LDAP) or 636 (LDAPS)
FortiClient download	Enabled		10443 (default)
Apache	HTTPS	TCP	443
SQL server			

Ensure the computer browser service is running. On Windows Server 2012 R2, the service is disabled by default. If this service is not active, FortiClient EMS cannot detect computers on the same network, even if they are available.

Deployment options

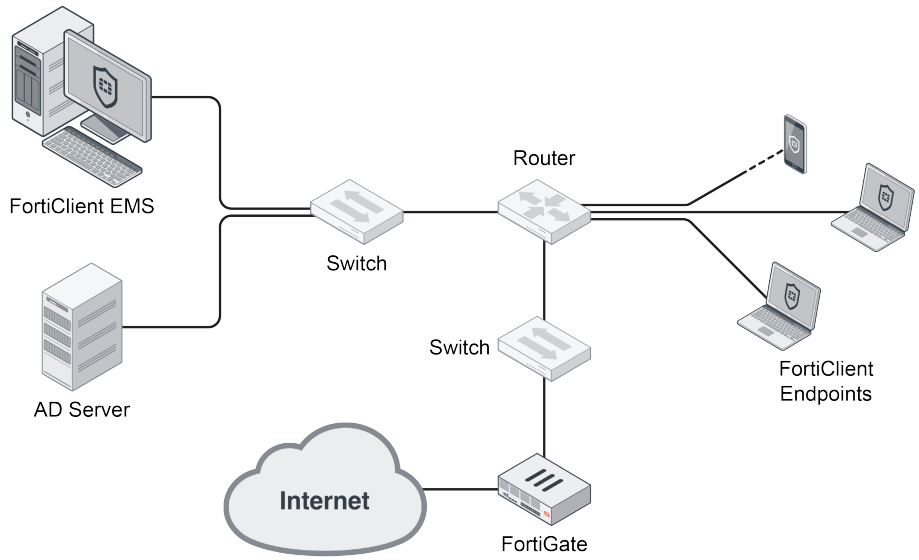
The following deployment options for EMS are supported: standalone or integrated with FortiGate.

Standalone



In standalone mode, a FortiGate is not required, and network access control (NAC) is not supported. In standalone mode, EMS deploys FortiClient software on endpoints, and FortiClient endpoints connect FortiClient Telemetry to EMS to receive configuration information from EMS. EMS is used to deploy, configure, and monitor FortiClient endpoints.

Integrated with FortiGate



In integrated mode, a FortiGate is required, and NAC is supported. In integrated mode, EMS deploys FortiClient software on endpoints, and FortiClient endpoints connect FortiClient Telemetry to FortiGate to receive compliance rules. FortiClient endpoints also connect to EMS to be managed. After FortiClient endpoints are connected, compliance rules are downloaded from FortiGate to the endpoint. EMS might also push a profile of FortiClient configuration information to endpoints. FortiClient endpoints are now managed, and NAC is enforced.

FortiClient uses the compliance rules from FortiGate to communicate whether the endpoint is compliant. If an endpoint fails to meet the compliance rules, the steps required to remain compliant are communicated. For more information, see the *FortiClient Administration Guide*.

Installation

For a complete endpoint solution, FortiClient should be installed on all endpoints, and FortiClient EMS should be installed for central management and provisioning of endpoints.

Following is a summary of how to install and start FortiClient EMS:

1. Download the installation file. See Downloading the installation file on page 8.
2. Install FortiClient EMS. See Installing FortiClient EMS on page 8.
3. Start FortiClient EMS and log in. See Starting FortiClient EMS and logging in on page 10.

For information about upgrading FortiClient EMS, see the FortiClient EMS *Release Notes*.

An instructional video on how to install, log in, and change your administrator password is available in the Fortinet Video Library.

Downloading the installation file

FortiClient EMS is available for download from the following location:

Fortinet Support website: https://support.fortinet.com/

You can also receive the installation file from a sales representative.

The following installation file is available for FortiClient EMS:

`FortiClientEnterpriseManagement_1.2.5.<build>_x64.exe`

For information about obtaining FortiClient EMS, contact your Fortinet reseller.

Installing FortiClient EMS

The FortiClient EMS installation package includes:

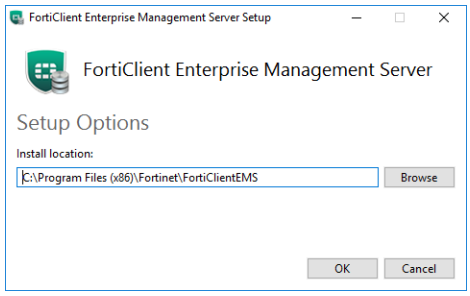
- FortiClient EMS
- Microsoft SQL Server 2014 Express Edition
- Apache HTTP server

Local administrator rights and Internet access are required to install FortiClient EMS.

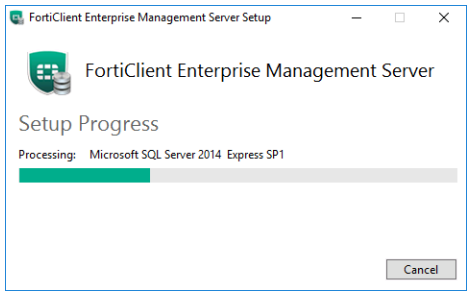
To install FortiClient EMS:

1. If you are logged into the system as an administrator, double-click the downloaded installation file.
   If you are not logged in as an administrator, right-click the installation file, and select *Run as administrator*.
2. If applicable, select *Yes* in the *User Account Control* window to allow the program to make changes to your system.
3. In the installation window, select *I agree to the license terms and conditions* if you agree with the license terms and conditions. If you do not agree, you cannot install the software.

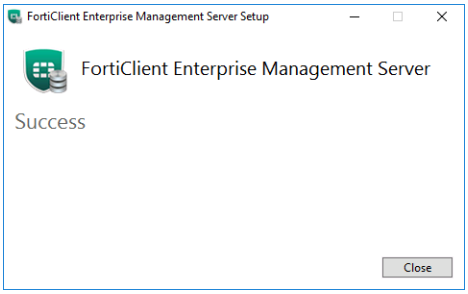
4. (Optional) Click *Options* to specify a custom directory for the FortiClient EMS installation.



   a. Click *Browse* to locate and select the custom directory.
   b. Click *OK* to return to the installation wizard.
5. Click *Install*.
   The installation may take 30 minutes or longer. It may appear to stop at times, but this is only because certain steps in the installation process take longer than others.



6. When the program has installed correctly, the *Success* window displays. Click *Close*.



A *FortiClient Enterprise Management Server* icon is added to the desktop.

Extending license expiries

You can apply multiple licenses to your FortiClient EMS to extend the license expiry. For example, consider you purchase two one-year licenses for FortiClient EMS. After you register and apply the first license, FortiClient EMS has an expiry date of August 1, 2018. You can register and apply the second license as a renewal, after which FortiClient EMS has an expiry date of August 1, 2019.

Note you must upload the second license file to FortiClient EMS using the GUI. Registering the license does not automatically update the license expiry in FortiClient EMS.

Using a second license to extend the license expiry date does not increase the number of licensed clients. To increase the number of licensed clients, contact Fortinet Support for a co-term contract.

For details, see the *FortiClient EMS Administration Guide*.

Starting FortiClient EMS and logging in

FortiClient EMS runs as a service on Windows computers.

To start FortiClient EMS:

1. Double-click the *FortiClient Enterprise Management Server* icon.
2. Sign in with the username *admin* and no password.
3. Change the username and password by going to *Administration* > *Administrators*.
4. Configure FortiClient EMS by going to *System Settings*.

Accessing FortiClient EMS remotely

You can access FortiClient EMS remotely using a web browser instead of the GUI.

To enable remote access to FortiClient EMS:

1. Go to *System Settings* > *Server*.
2. Enable *Remote HTTPS access*.
3. If desired, in the *Custom hostname* box, type the host name or IP address. Otherwise, the *Pre-defined hostname* is used.
4. If desired, select the *Redirect HTTP request to HTTPS* checkbox. If this option is enabled, if you attempt to remotely access EMS at *http://<server_name>*, this is automatically redirected to *https://<server_name>*.
5. Click *Save*.

To remotely access FortiClient EMS:

- To access EMS from the EMS server, visit `https://localhost`
- To access the server remotely, use the server's hostname: `https://<server_name>`
  Ensure you can ping `<server_name>` remotely. This can be achieved by adding it into a DNS entry or to the Windows hosts file. You may have to modify the Windows firewall rules to allow the connection.

Endpoint Management Setup

This section describes how to set up FortiClient EMS for endpoint management. It provides an overview of using FortiClient EMS and FortiClient EMS integrated with FortiGate.

When FortiClient EMS is integrated with FortiGate, you can use gateway IP lists to help FortiClient endpoints connect to FortiClient EMS and FortiGate. You can also import FortiClient profiles from FortiGate to FortiClient EMS.

FortiClient EMS

Following is a summary of how to use FortiClient EMS without FortiGate:

1. Configure user accounts. See Configuring user accounts on page 13.
2. Add domains and/or discover local endpoints. See Adding endpoints on page 14
3. Add a FortiClient installer to EMS. See Adding FortiClient installers on page 17.
4. Create an endpoint profile and select a FortiClient installer. See Creating profiles to deploy FortiClient on page 19.

You can use FortiClient EMS with an Active Directory server to install and upgrade FortiClient (Windows) on endpoints before and after endpoints connect Telemetry to EMS. You can use FortiClient EMS with workgroups only to upgrade FortiClient (Windows) on endpoints after they connect Telemetry to EMS and FortiClient connects to FortiClient EMS. When using workgroups, you must separately install FortiClient (Windows) on endpoints. See the *FortiClient EMS Administration Guide*.

You can use FortiClient EMS to replace, upgrade, and uninstall FortiClient (Mac OS X) after they connect Telemetry to EMS and FortiClient connects to FortiClient EMS. You cannot use FortiClient EMS to initially deploy FortiClient (Mac OS X) and must separately install it on endpoints. See the *FortiClient EMS Administration Guide*.

5. Prepare Windows endpoints for FortiClient deployment. See Preparing Windows endpoints for FortiClient deployment on page 22.

   You must also prepare the Windows AD server for deployment. See the *FortiClient EMS Administration Guide*.
6. Assign a profile to a workgroup, domain, endpoint group, or organizational group. See Assigning profiles to endpoints on page 23.

   Depending on the selected profile's configuration, FortiClient is installed on the endpoints to which the profile is applied.

   After FortiClient installation, the endpoint user must connect FortiClient Telemetry to FortiGate or FortiClient EMS to receive the profile configuration and complete endpoint management setup. See Connecting manually from FortiClient on page 15.
7. View the endpoint status. See Viewing endpoints on page 23.

FortiClient EMS integrated with FortiGate

Following is a summary of how to use FortiClient EMS when integrated with FortiGate:

1. Configure user accounts. See Configuring user accounts on page 13.
2. Add domains and/or discover local endpoints. See Adding endpoints on page 14
3. Create gateway IP lists. See Creating gateway IP lists on page 16.
4. Assign the lists to domains or workgroups. See Assigning gateway IP lists to endpoints on page 17.
   Alternately, you can add a FortiClient Telemetry gateway IP list to a custom FortiClient installer using the FortiClient Configurator tool.
5. Add a FortiClient installer to EMS. See Adding FortiClient installers on page 17.
6. Create an endpoint profile and select a FortiClient installer. See Creating profiles to deploy FortiClient on page 19.

You can use FortiClient EMS with an Active Directory server to install and upgrade FortiClient (Windows) on endpoints before and after endpoints connect Telemetry to EMS. You can use FortiClient EMS with workgroups only to upgrade FortiClient (Windows) on endpoints after they connect Telemetry to EMS and FortiClient connects to FortiClient EMS. When using workgroups, you must separately install FortiClient (Windows) on endpoints. See the *FortiClient EMS Administration Guide*.

You can use FortiClient EMS to replace, upgrade, and uninstall FortiClient (Mac OS X) after they connect Telemetry to EMS and FortiClient connects to FortiClient EMS. You cannot use FortiClient EMS to initially deploy FortiClient (Mac OS X) and must separately install it on endpoints. See the *FortiClient EMS Administration Guide*.

7. Prepare Windows endpoints for FortiClient deployment. See Preparing Windows endpoints for FortiClient deployment on page 22.
   You must also prepare the Windows AD server for deployment. See the *FortiClient EMS Administration Guide*.
8. Assign a profile to a workgroup, domain, endpoint group, or organizational group. See Assigning profiles to endpoints on page 23.
   Depending on the selected profile's configuration, FortiClient is installed on the endpoints to which the profile is applied.
   After FortiClient installation, the endpoint user must connect FortiClient Telemetry to FortiGate or FortiClient EMS to receive the profile configuration and complete endpoint management setup. See Connecting manually from FortiClient on page 15.
9. View the endpoint status. See Viewing endpoints on page 23.

Configuring user accounts

You can configure users to have no access or administrator access to FortiClient EMS. You can configure local Windows users, LDAP users, or local Windows users and LDAP users.

For local Windows users, the user list is derived from the server where FortiClient EMS is installed. If you want to add more users, you must add them to the server.

For LDAP users, you must add an LDAP server to FortiClient EMS, then configure users.

To add an LDAP server:

1. Go *Administration* > *User Server*.
2. Configure the options, and click *Test*.
3. If the test is successful, click *Save*.

To configure users:

1. Go to *Administration* > *Administrators*.
2. Click *Add* from the toolbar.
3. In the *User* list, select *Windows* or *LDAP*.
   The *LDAP* option is available only after you add an LDAP server to FortiClient EMS.
4. Select the user's specific domain access.
5. Configure the permissions.
6. Click *Save*.

Adding endpoints

You can add endpoints using an Active Directory service. Endpoints are also added when endpoint users manually connect FortiClient Telemetry to FortiClient EMS.

Adding endpoints using an Active Directory domain server

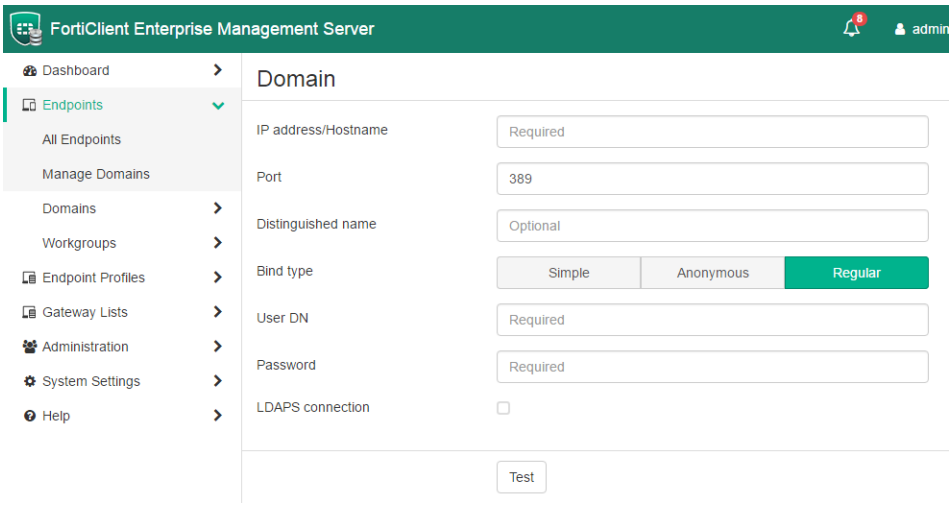
Endpoints can be manually imported from an Active Directory (AD) domain server. You can import and synchronize information about computer accounts with an LDAP or LDAPS service. You can add endpoints by identifying endpoints that are part of an AD domain server.

An instructional video on how to add a domain is available in the Fortinet Video Library.

You can add the entire domain or an organizational unit (OU) from the domain.

To add endpoints using an Active Directory domain service:

1. Click *Endpoints* > *Manage Domains* > *Add*. The *Domain* pane displays.



2. Configure the following options:

IP address/Hostname	Type the IP address or name.
Port	Type the port number.
Distinguished name	Type the distinguished name (optional).
Bind type	Select the bind type: *Simple*, *Anonymous*, or *Regular*. When you select *Regular*, enter the *User DN* and *Password*.
User DN	Available when *Bind Type* is set to *Regular*. Type the user DN.
Password	Available when *Bind Type* is set to *Regular*. Type the user password.
Show Password	Available when *Bind Type* is set to *Regular*. Turn on and off to show or hide the password.
LDAPS connection	Turn on to enable a secure connection protocol when *Bind Type* is set to *Regular*.

3. Click *Test* to test the domain settings connection.
4. If the test is successful, select *Save* to save the new domain. If not, correct the information as required then test the settings again.

Connecting manually from FortiClient

Endpoint users can manually connect FortiClient Telemetry to FortiClient EMS by specifying the IP address for FortiClient EMS in FortiClient Console. This process is sometimes called registering FortiClient to FortiClient EMS.

To connect FortiClient Telemetry to FortiClient EMS:

1. In FortiClient Console on the endpoint, go to the *Compliance* tab.
2. In the *FortiGate or EMS* box, type the IP address for EMS, and click *Connect*.
   FortiClient connects to FortiClient EMS.

For information about FortiClient, see the *FortiClient Administration Guide* available on docs.fortinet.com/forticlient/admin-guides.

The FortiClient Telemetry gateway port may be appended to the gateway IP list address on FortiClient and separated by a colon. When the port is not provided, FortiClient attempts to connect to the IP address given using the default port. The default connection port in FortiClient 5.2 is 8010 and in FortiClient 5.4 is 8013. By default, FortiClient EMS listens for connection on port 8013.

Creating gateway IP lists

Gateway IP lists are useful when using FortiClient EMS integrated with FortiGate. If using FortiClient EMS without FortiGate, you are not required to use gateway IP lists.

You can create one or more gateway IP lists. Each list can contain IP addresses for multiple FortiGate units.

To create gateway IP lists:

1. Go to *Gateway IP Lists* > *Manage Gateway Lists*.
2. Click the *Add* button.

3. Configure the following:

Name		Enter the list name.
Comment		Enter additional comments (optional).
IP addresses/hostnames		Enter the IP address and port for FortiGates using the following format: IP:port. You can also use an FQDN. Press the *Enter* key to add additional IP addresses.
Connect to local subnets only		Enable to only allow to connect to local subnets.
Use connection key		Enable the connection key endpoints can use to connect to FortiGate units.
	New connection key	Enter the connection key.
	Confirm new connection key	Reenter the connection key to confirm.
Monitored by EMS		Select an option from the dropdown list. Users can configure this IP address in *System Settings* > *Server*.

4. Click *Save*.

Assigning gateway IP lists to endpoints

After creating a gateway IP list, you can assign the list to endpoints. When you assign the IP list and FortiClient Telemetry data registration process has started, the endpoint connects to a FortiGate or EMS, based on the gateway IP list.

To assign gateway IP lists to endpoints:

1. Go to *Endpoints*.
2. Right-click a domain or workgroup, and select *Assign gateway list*.
3. Select the desired list or create a new gateway IP list.

Adding FortiClient installers

When you add a FortiClient installer to FortiClient EMS, you can specify what FortiClient features to include in the installer for the endpoint. You can include a feature in the installer, then disable the feature in the profile. Because the feature is included in the installer, you can update the profile later to enable the feature on the endpoint.

When you add a FortiClient installer to FortiClient EMS, an installer for the Windows operating system and an installer for the OS X operating system are added to FortiClient EMS.

After you add a FortiClient installer to FortiClient EMS, you cannot edit it. You can delete the installer from FortiClient EMS, and edit the installer outside of FortiClient EMS. You can then add the edited installer to FortiClient EMS.

To add FortiClient installers:

1. Go to *Administration* > *Software Management*.
2. Click *Add*.
3. On the *General* tab, set the following options:

Name	Type the FortiClient installer's name.
Notes	(Optional) Type any notes about the FortiClient installer.
Version	Select the FortiClient version to install. Click *Upload* to add a custom FortiClient installer.
Patch version	Select the specific FortiClient patch version to install.
Keep updated to the latest patch	Select to enable FortiClient to automatically update to the latest patch release when FortiClient is installed on an endpoint. This field is only available for the latest FortiClient version FortiClient EMS can access from FortiGuard. This option is not available if an older FortiClient version is selected.

4. Click *Next*. On the *Features* tab, set the following options:

Security Fabric Agent (Mandatory Feature)	Enabled by default and cannot be disabled. Installs FortiClient with Telemetry and Vulnerability Scanning enabled.
Secure Access Architecture Components	Enable to install FortiClient with SSL VPN and IPsec VPN enabled. Disable to omit SSL VPN and IPsec VPN support from the FortiClient installer.
Advanced Persistent Threat (APT) Components	Enable to install FortiClient with APT components enabled. Disable to omit APT components from the FortiClient installer. Includes FortiSandbox detection and quarantine features.
Additional Security Features	Enable to select one, two, or all of the following features: • AntiVirus • Web Filtering • Application Firewall • Single Sign-On mobility agent Disable to exclude the features from the FortiClient installer.
Enable automatic registration	Enable to configure FortiClient to automatically connect Telemetry to EMS or FortiGate after FortiClient is installed on the endpoint. Disable to turn off this feature and require endpoint users to manually connect Telemetry to EMS or FortiGate.

Enable desktop shortcut	Enable to configure the FortiClient installer to create a desktop shortcut on the endpoint.
Enable start menu shortcut	Enable to configure the FortiClient installer to create a Start menu shortcut on the endpoint.

5. Click *Next*. On the *Telemetry* tab, set the following options:

EMS	Click *EMS* to configure the FortiClient installer to connect Telemetry to EMS.
FortiGate	Click *FortiGate*, and select the name of the gateway IP list to use. The gateway IP list defines the IP address for FortiGate and includes the IP address for EMS. You must define a FortiClient Telemetry gateway IP list to select FortiGate. If you have not created a list, the *No Gateway IPs have been defined* dialog box is displayed, and you can click *OK* to create a list.

6. Click *Save*. The FortiClient installer is added to FortiClient EMS and displays on the *Software Management* pane.

If the *Sign software packages* option is enabled in *System Settings* > *Server*, Windows installers display as being from the publisher specified in the certificate file. See the *FortiClient EMS Admin Guide*.

Configuring profiles

When you install FortiClient EMS, a default profile is created. This profile is applied to any groups you create. The default profile is designed to provide effective levels of protection. To use specific features, such as application firewall, create a new profile or change the default profile.

Consider the following when creating profiles:

- Use default settings within a profile.
- Consider the endpoint's role when changing the default profile or creating new profiles.
- Create a separate group and profile for endpoints requiring long-term special configuration.
- Use FortiClient EMS for all central profile settings, and set options for within the group instead of for the endpoint itself when possible.

Creating profiles to deploy FortiClient

You must create a new profile to deploy FortiClient to endpoints. You cannot add a FortiClient installer to the default profile.

You must add FortiClient installers to FortiClient EMS before you can select the installers in a profile. See Adding FortiClient installers on page 17.

The selected FortiClient installer in a profile controls what tabs are displayed for configuration in the profile. Only the tabs for the features in the selected installer are displayed for configuration in the profile. For example, if the installer

includes only the VPN feature, only the *VPN* tab is displayed for you to configure. The *System Settings* tab always displays.

You can disable a feature included in the installer, then enable the feature in the profile later. For example, if the installer includes the Web Filter and VPN features, you can disable the Web Filter feature and keep the VPN feature enabled. When FortiClient is installed on the endpoint, the Web Filter is installed, but disabled.

To create profiles for FortiClient deployment:

1. Go to *Endpoint Profiles* > *Manage Profile*, and click the *Add* button.
2. On the *Deployment* tab, enable *FortiClient Deployment*. The FortiClient deployment options display.
3. Set the following options on the *Deployment* tab:

Action		
	Assign an	Click *Installer*.
	Installer	In the *Installer* list, select a FortiClient installer. If you have not added a FortiClient installer to FortiClient EMS, see Adding FortiClient installers on page 17. The selected FortiClient installer affects what tabs display for configuration. Only tabs related to features enabled in the FortiClient installer display for configuration.
Schedule		
	Start At	Specify what time to start installing FortiClient on endpoints.
	Prompt User If a Reboot Is Needed During Installation	Enable to prompt the end user if a reboot of the endpoint is needed. Disable to reboot the endpoint without prompting the user. If no endpoint user is logged into FortiClient, the endpoint reboots without prompt.
Credentials		
	Username	Type the username to perform deployment on AD. You must enter the admin credentials for the AD in the profile. Enter the appropriate credentials in the profile to assign to the AD. The credentials allow EMS to install FortiClient on endpoints using AD. If the credentials are wrong, the installation fails, and an error displays in EMS.
	Password	Type the password to perform deployment on AD.

4. Set the options on the remaining tabs.
5. Click *Save*.

Importing FortiGate profiles

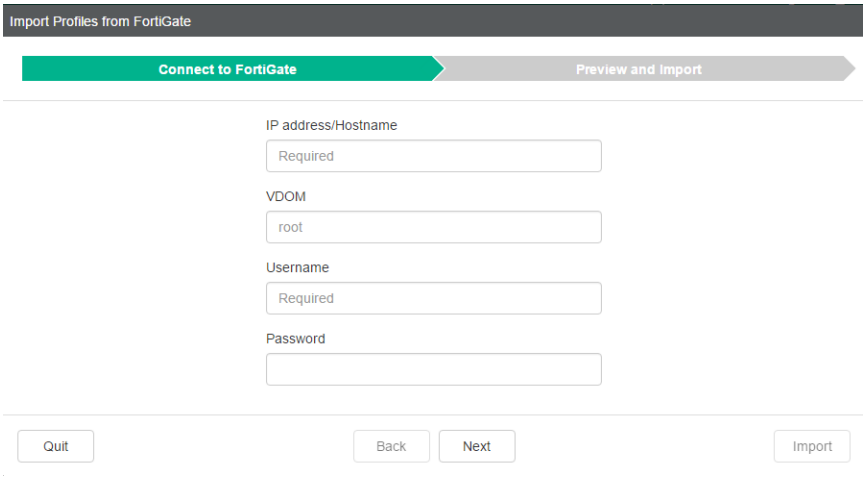
In FortiOS, endpoint profiles are called FortiClient profiles. You can import a FortiClient profile into EMS, then edit the profile in FortiClient EMS to add a FortiClient installer or add configuration information that supports the FortiGate

compliance rules.

To import profiles successfully from FortiOS to FortiClient EMS, FortiGate must have the HTTPS port open. In FortiOS, go to *Network* > *Interfaces* > *Restrict Access* > *Enable checkbox for HTTPS*.

To import profiles:

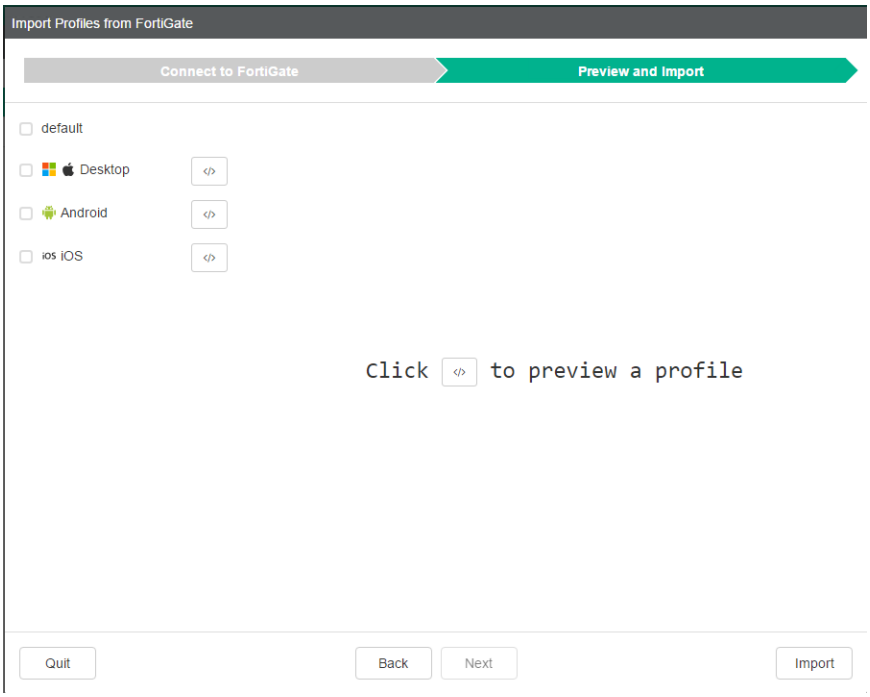
1. Click *Endpoint Profiles* > *Manage Profiles* > *Import*. The *Import Profiles from FortiGate* window opens.



2. Complete the following options, and click *Connect*.

IP address/Hostname	Enter the IP address and port of the FortiGate from which the profile is being imported, in the format: `<ip address>:<port>`.
VDOM	Enter a VDOM name from the FortiGate if applicable.
Username	Enter the FortiGate's login username.
Password	Enter the FortiGate's login password.

The list of FortiClient profiles configured on the FortiGate displays.



Under each profile name is the list of profiles created for different operating systems, such as desktops running a Windows or Mac operating system or devices running an Android operating system. For example, under the default profile, *Desktop*, *Android* and *iOS* profiles are listed. You can click the </> icon beside each profile to preview the settings in XML format.

3. Select the profiles to import into EMS and click *Import*.

   Select the name of the profile to import all profiles for it into EMS. You can also clear the checkbox beside the profiles you do not want to import into EMS. For example, you can import the desktop and iOS profiles, but not the Android profile for a given profile name.

   The selected profiles are imported into EMS and display under the *Endpoint Profiles* pane in a group named after the FortiGate from which they were imported.
4. In the *Endpoint Profiles* page, select an imported profile to edit it.

   The options configured in the profile by the FortiGate administrator are read-only compliance rules. You cannot change them. You can edit additional options to provide configuration information to support the compliance rules. You can also add a FortiClient installer to the profile by using the *Deployment* tab. Custom installers can be created. See Adding FortiClient installers on page 17.
5. Edit the options on the tabs.
6. Click *Save Profile*.

Preparing Windows endpoints for FortiClient deployment

The following services must be enabled and configured on each Windows endpoint before FortiClient is deployed to them:

- Task Scheduler: Automatic
- Windows Installer: Manual
- Remote Registry: Automatic

The Windows Firewall must be configured to allow the following inbound connections:

- File and Printer Sharing (SMB-In)
- Remote Scheduled Tasks Management (RPC)

For AD group deployments, an AD administrator account is required. For non-AD deployments, the installer URL can be shared with users, who can then download and install FortiClient manually. You can locate the installer URL in *Software Management*. Go to *Administration* > *Software Management*.

Assigning profiles to endpoints

After creating the profile, you can assign the profile to domains or workgroups. When you assign the profile to domains or workgroups, the profile settings are automatically pushed to the endpoints in the domain or workgroup.

If you do not assign a profile to a specific domain or workgroup, the default profile is automatically applied.

To assign profiles:

1. Go to *Endpoints*.
2. Right-click a domain or group, select *Assign profile*, then the profile. A confirmation dialog box displays.
3. Click *Yes*. The profile is assigned.

Viewing endpoints

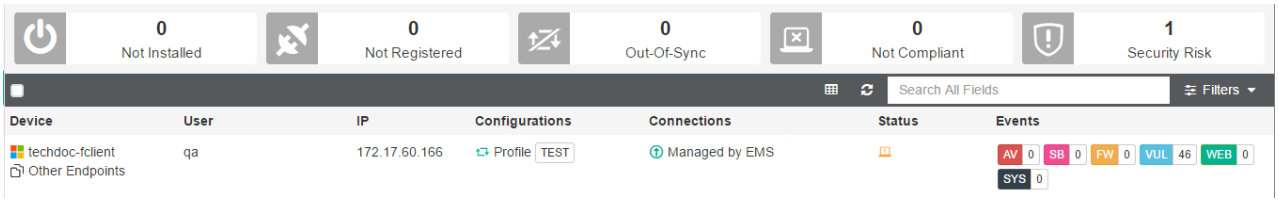
After you add endpoints to FortiClient EMS, you can view the list of endpoints in a domain or workgroup in the *Endpoints* pane. You can also view details about each endpoint in the *Client Details* pane and use filters to access endpoints with specific qualities.

Viewing the Endpoints content pane

You can view information about endpoints on the *Endpoints* content pane.

To view the Endpoints content pane:

1. Go to *Endpoints*, and select *All Endpoints*, a domain, or workgroup.
   The list of endpoints in FortiClient EMS, a quick status bar, and a toolbar display in the content pane.

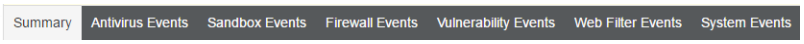


Not Installed	Number of endpoints that do not have FortiClient installed. Click to display the list of endpoints without FortiClient installed.
Not Registered	Number of endpoints not registered to FortiClient EMS or FortiGate. Click to display the list of unregistered endpoints.
Out-Of-Sync	Number of endpoints with an out-of-sync profile. Click to display the list of endpoints with out-of-sync profiles.
Not Compliant	Number of endpoints not compliant with the FortiGate compliance rules. Click to display the list of not compliant endpoints.
Security Risk	Number of endpoints that are a security risk. Click to display the list of endpoints.
Checkbox	Click to select all endpoints displayed in the content pane.
Show/Hide Heading	Click to hide and display the following column headings: *Device*, *User*, *IP*, *Configurations*, *Connections*, *Status*, and *Events*.
Refresh	Click to refresh the list of endpoints in the content pane.
Search All Fields	Type a value and press *Enter* to search for the value in the list of endpoints.
Filters	Click to display and hide filters you can use to filter the list of endpoints.
Device	Visible when headings are displayed. Displays an icon to represent the operating system on the endpoint and the device name.
User	Visible when headings are displayed. Displays the name of the user logged into the endpoint.
IP	Visible when headings are displayed. Displays the endpoint's IP address.
Configurations	Visible when headings are displayed. Displays the name of the profile assigned to the endpoint and the profile's synchronization status.
Connections	Visible when headings are displayed. Displays whether the endpoint is connected to FortiClient EMS or FortiGate and the connection status of *Online*, *Offline*, or *Not Registered*.
Status	Visible when headings are displayed. Displays one of the following compliance statuses for the endpoint. • Compliant • Not compliant • Not participating in compliance • Quarantined • Excluded • Not registered • Not installed
Events	Visible when headings are displayed. Displays FortiClient events for the endpoint.

2. Click an endpoint to display its details in the content pane.
   The following dropdown lists display in the toolbar for the selected endpoint:

Checkbox	Click to select and deselect all endpoints in the content pane. You can then select or clear the checkbox for individual endpoints to fine-tune the list of selected endpoints.
Scan	Click to start a Vulnerability or AntiVirus scan on the selected endpoint.
Patch	Click to patch all critical and high vulnerabilities on the selected endpoint. Choose one of the following options: • Selected Vulnerabilities on Selected Clients • Selected Vulnerabilities on All Affected Clients • All Critical and High Vulnerabilities
Action	Click to perform one of the following actions on the selected endpoint: • Upload FortiClient Logs • Request Diagnostic Results • Update Signatures • Re-register • De-register • Register • Quarantine • Un-quarantine • Exclude from Management • Mark as Uninstalled • Delete Device

The following tabs are available in the content pane toolbar when you select an endpoint:



Summary		
	<user name>	Displays the name of the user logged into the selected endpoint. Also displays the user's avatar, email address, and phone number if these are provided to FortiClient on the endpoint. If the user's LinkedIn, Google, Salesforce, or other cloud app account is linked in FortiClient, the username from the cloud application displays.
	Device	Displays the selected endpoint's device name.
	OS	Displays the selected endpoint's operating system and version number.
	IP	Displays the selected endpoint's IP address.
	MAC	Displays the selected endpoint's MAC address.

	Last Seen	Displays the last date and time that FortiClient sent a keep-alive message to EMS. This information is useful if FortiClient is offline because it indicates when the last keep-alive message occurred.
	Location	Displays whether the selected endpoint is onnet or offnet.
	Connection	Displays when the selected endpoint is connected to FortiClient EMS or FortiGate. Also displays the connection status.
	Configuration	Displays the following information for the selected endpoint: • Profile: Name of the profile assigned to the selected endpoint • Installer: Name of the FortiClient installer used for the selected endpoint. Displays *Not Assigned* if no FortiClient installer has been assigned to the selected endpoint. • IP List: Name of the gateway IP list used for the selected endpoint. Displays *Not Assigned* if no gateway IP list has been assigned to the selected endpoint. • FortiClient Version: FortiClient version installed on the selected endpoint.
	Compliance	Displays if the endpoint is compliant. If the endpoint is not compliant, displays the features for which FortiClient is not compliant.
	Features	Displays which features are enabled for FortiClient.
Antivirus Events		
	Date/Time	Displays the antivirus event's date and time.
	Message	Displays the antivirus event's message.
Sandbox Events		
	Date/Time	Displays the sandbox event's date and time.
	Message	Displays the sandbox event's message.
Firewall Events		
	Date/Time	Displays the firewall event's date and time.
	Message	Displays the firewall event's message.
Vulnerability Events		
	Vulnerability	Displays the vulnerability's name. For example, *Security update available for Adobe Reader*.
	Category	Displays the vulnerability's category. For example, *Third Party App*.
	Application	Displays the name of the application with the vulnerability.
	Severity	Displays the vulnerability's severity.

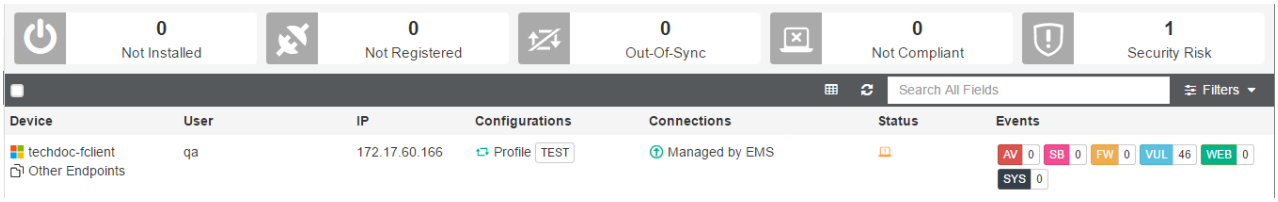
	FortiGuard ID	Displays the FortiGuard ID number. If you click the FortiGuard ID number, it redirects you to FortiGuard where further information is provided if available.
	Bulletin	Displays a link to a bulletin about the software vulnerability.
Web Filter Events		
	Date/Time	Displays the web filter event's date and time.
	Message	Displays the web filter event's message.
System Events		
	Date/Time	Displays the system event's date and time.
	Message	Displays the system event's message.

Using the quick status bar

You can use the quick status bar to quickly display filtered lists of endpoints on the *Endpoints* content pane.

To use the quick status bar:

1. Go to *Endpoints*.
2. Click *All Endpoints*, a domain, or workgroup.
   The list of endpoints and quick status bar display.



3. Click one of the following buttons in the quick status bar:
   - Not Installed
   - Not Registered
   - Out-Of-Sync
   - Not Compliant
   - Security Risk

   The list of affected endpoints displays.
4. Click an endpoint to display its details.
5. In the *Events* column, click the *AV <number>, SB <number>, FW <number>*, *VUL<number>*, *WEB <number>* and *SYS<number>* buttons to display the associated tab of details for the selected endpont.
6. Click the *Total* button to clear the filters.
   The unfiltered list of endpoints displays.

Viewing endpoint details

You can view each endpoint's details on the *Endpoints* content pane. For a description of the options on the *Endpoints* content pane, see Viewing the Endpoints content pane on page 23.

To view endpoint details:

1. Go to *Endpoints*, and select *All Domains*, a domain, or workgroup.
   The list of endpoints for the selected domain or workgroup displays.
2. Click an endpoint to display details about it in the content pane.
   Details about the endpoint display in the content pane.